CLAIM SET AS AMENDED

1-12. (Canceled)

13. (Currently Amended) A method for copy protection, comprising:

generating a partially decrypted data unit, the partially decrypted data unit including two portions, one of the two portions is encrypted having a protection level different from the other of the two portions; and

transferring the partially decrypted data unit to a target device for further decrypting based on information used in the step of generating the partially decrypted data unit; and

further comprising the steps of:

registering a computer with a data server;

transferring encrypted data from the data server to the computer, the computer generating the partially decrypted data unit in a first decryption unit of the computer; and

using a second decryption unit of the target device to further decrypt the partially decrypted data unit based on the information used in the step of generating the partially decrypted data unit.

14. (Previously Presented) The method of claim 13, wherein the two portions having the different protection levels are spaced apart at a predetermined interval on the data unit.

15. (Previously Presented) The method of claim 14, further comprising the step of storing the partially decrypted data unit in a data storage medium or a digital data player.

16. (Previously Presented) The method of claim 14, further comprising the step of decrypting a remainder of the partially decrypted data unit in the target device.

17. (Previously Presented) The method of claim 13, wherein the data unit is partially decrypted based on a predetermined encryption key.

18. (Previously Presented) The method of claim 15, further comprising the step of reading the partially decrypted stored data unit from the data storage medium or the digital data player and reproducing the data unit at the request of a user.

19. (Previously Presented) The method of claim 18, further comprising the step of decrypting the data unit based on a predetermined encryption key, and outputting the decrypted data unit to an output line.

20. (Previously Presented) The method of claim 14, wherein the predetermined interval is a multiple or divisor of a buffer size.

21-27. (Canceled)

28. (Currently Amended) The method of ~~claim 38~~ claim 13, wherein the step of partially decrypting the encrypted data unit in the computer is performed at a plurality of locations spaced apart at a predetermined interval on the partially decrypted data unit.

29. (Currently Amended) The method of ~~claim 38~~ claim 13, further comprising the step of storing the partially decrypted data unit in a data storage medium or a digital data player.

30. (Canceled)

31. (Currently Amended) The method of ~~claim 38~~ claim 13, wherein the data unit received by the target device is partially decrypted based on a predetermined encryption key.

32. (Previously Presented) The method of claim 29, further comprising the step of reading the partially decrypted stored data unit from the data storage medium and reproducing the partially decrypted data unit upon request of a user.

33. (Previously Presented) The method of claim 32, further comprising the steps of:

sending the partially decrypted digital data unit to the digital data player;

decrypting the reencrypted data unit based on a predetermined encryption key; and

outputting the decrypted data unit to an output line of the digital data player.

34-35. (Canceled)

36. (Currently Amended) The method of ~~claim 38~~ claim 13, further comprising the steps of:

partially decrypting the encrypted data unit in the computer is performed independently of operating the second decryption unit in the target device.

37-39. (Canceled)

40. (Currently Amended) A method for copy protection, comprising:

receiving a data unit that has been encrypted based on a predetermined encryption key;

identifying whether or not the received data unit needs to be protected;

generating an encrypted data unit having a different encryption level or method from one used to encrypt the data unit, based on a result of the identifying step; and

transferring the generated encrypted data unit having the different encryption level or method to a target device for decrypting based on information used in the step of generating the ~~differently~~ encrypted data unit ~~data unit~~; and

further comprising the steps of:

registering a computer with a data server;

transferring the data unit from the data server to the computer;

using a first decryption unit of the computer for generating the encrypted data unit having the different encryption level or method; and

using a second decryption unit of the target device for decrypting the generated encrypted data unit having the different encryption level or method based on the information used in the step of generating the generated encrypted data unit.

41. (Previously Presented) The method of claim 40, wherein the generated encrypted data unit includes two portions having the different protection levels spaced apart at a predetermined interval on the data unit.

42. (Previously Presented) The method of claim 41, further comprising the step of storing the generated encrypted data unit in a data storage medium or a digital data player.

43. (Previously Presented) The method of claim 41, further comprising the step of decrypting the generated encrypted data unit in the target device.

44. (Previously Presented) The method of claim 40, wherein the step of generating the encrypted data unit is based on a predetermined encryption key.

45. (Previously Presented) The method of claim 42, further comprising the step of reading the generated encrypted data unit from the data storage medium or the digital data player and reproducing the data unit at the request of a user.

46. (Previously Presented) The method of claim 45, further comprising the step of decrypting the data unit based on a predetermined encryption key, and outputting the decrypted data unit to an output line.

47. (Previously Presented) The method of claim 41, wherein the predetermined interval is a multiple or divisor of a buffer size.

48. (Currently Amended) A method for copy protection, comprising the steps of:

enabling a registration mode for inputting a user identification;

receiving a data unit from a storage device based on the inputted user identification information, wherein the data unit has been encrypted;

generating an encrypted data unit having a different encryption level or method from one used to encrypt the data unit; and

transferring the encrypted data unit <u>having the different encryption level or method</u> to a target device for decrypting based on information used in the step of generating the differently encrypted data unit<u>; and</u>

<u>further comprising the steps of:</u>

registering a computer with a data server;

transferring the data unit from the data server to the computer;

using a first decryption unit of the computer for generating the encrypted data unit having the different encryption level or method; and

using a second decryption unit of the target device for decrypting the generated encrypted data unit having the different encryption level or method based on the information used in the step of generating the generated encrypted data unit.

49. (Previously Presented) The method of claim 48, wherein the step of generating the encrypted data unit is performed at a plurality of locations spaced apart at a predetermined interval on the generated encrypted data unit.

50. (Previously Presented) The method of claim 48, further comprising the step of storing the generated encrypted data unit in a data storage medium or a digital data player.

51. (Previously Presented) The method of claim 48, wherein the data unit received by the target device is encrypted based on a predetermined encryption key.

52. (Previously Presented) The method of claim 49, further comprising the step of reading the generated encrypted data unit from the data storage medium and reproducing the generated encrypted data unit upon request of a user.

53. (Previously Presented) The method of claim 52, further comprising the steps of:

sending the generated encrypted data unit to the digital data player;

decrypting the generated encrypted data unit based on a predetermined encryption key; and

outputting the decrypted data unit to an output line of the digital data player.

54. (Previously Presented) The method of claim 48, wherein the step of generating the encrypted data unit is performed independently of decrypting the generated encryption unit in the target device.

55. (Currently Amended) A method for encrypting a digital data file, comprising:

receiving a data file from a digital data server, the data file having been encrypted in the digital data server based on a predetermined encryption key;

decrypting the data file using the predetermined encryption key;

identifying whether or not the received data file needs to be protected;

reencrypting the decrypted data file on the basis of the identified result; and

transferring the reencrypted data file to a target device,

wherein the reencrypted data file has a different level of encryption as compared to that of the received data file that was encrypted in the digital data server; and

further comprising the steps of:

registering a computer with the digital data server;

transferring the data file from the digital data server to the computer;

using a first decryption unit of the computer for generating the reencrypted data file having the different level of encryption; and

using a second decryption unit of the target device to decrypt the reencrypted data file having the different level of encryption based on the information used in the step of reencrypting the decrypted data file.